FedCIRC

Network-Based Intrusion Detection Routers, Firewalls, and Network Monitoring

Jeffrey J. Carpenter

Intrusion Detection Workshop

Gaithersburg, Maryland

April 23-24, 1997

Technical Acknowledgments

- Jed Pickel, FedCIRC East
- Scott Denton, FedCIRC West

Introduction

What is network-based intrusion detection?

Topics

- Network monitoring
- Firewalls
- Routers

Topics

➤
- Network monitoring
- Firewalls
- Routers

Network Monitoring

- Why use network monitoring?
- Types of monitoring
- Know your network access points
- Intruder and user profiling
- Know what to look for in your log files

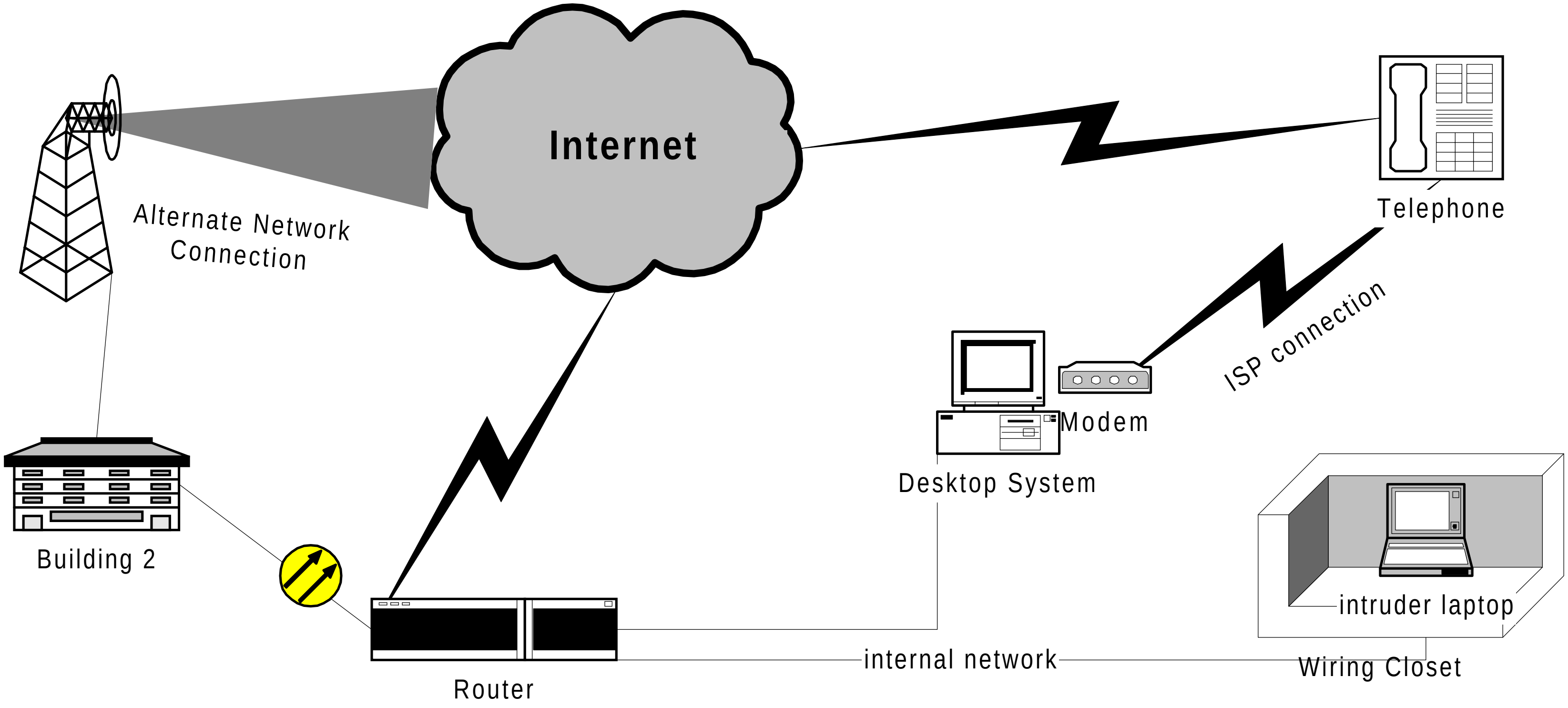
Why Use Network Monitoring?

- Network-based vs. host-based
  - host monitoring alone is not sufficient
  - network monitoring can focus on specific locations on a network
  - does not require modification of individual host software
- Network-based monitoring can be used to detect
  - break-in attempts
  - vulnerability exploits
  - intruder scans
  - automated attacks
  - the presence of new machines on network

Know your network access points

- Know your network topology
- Networks can be accessed from multiple access points
  - routers
  - modems
  - physical network (such as wiring closets)

Access Points



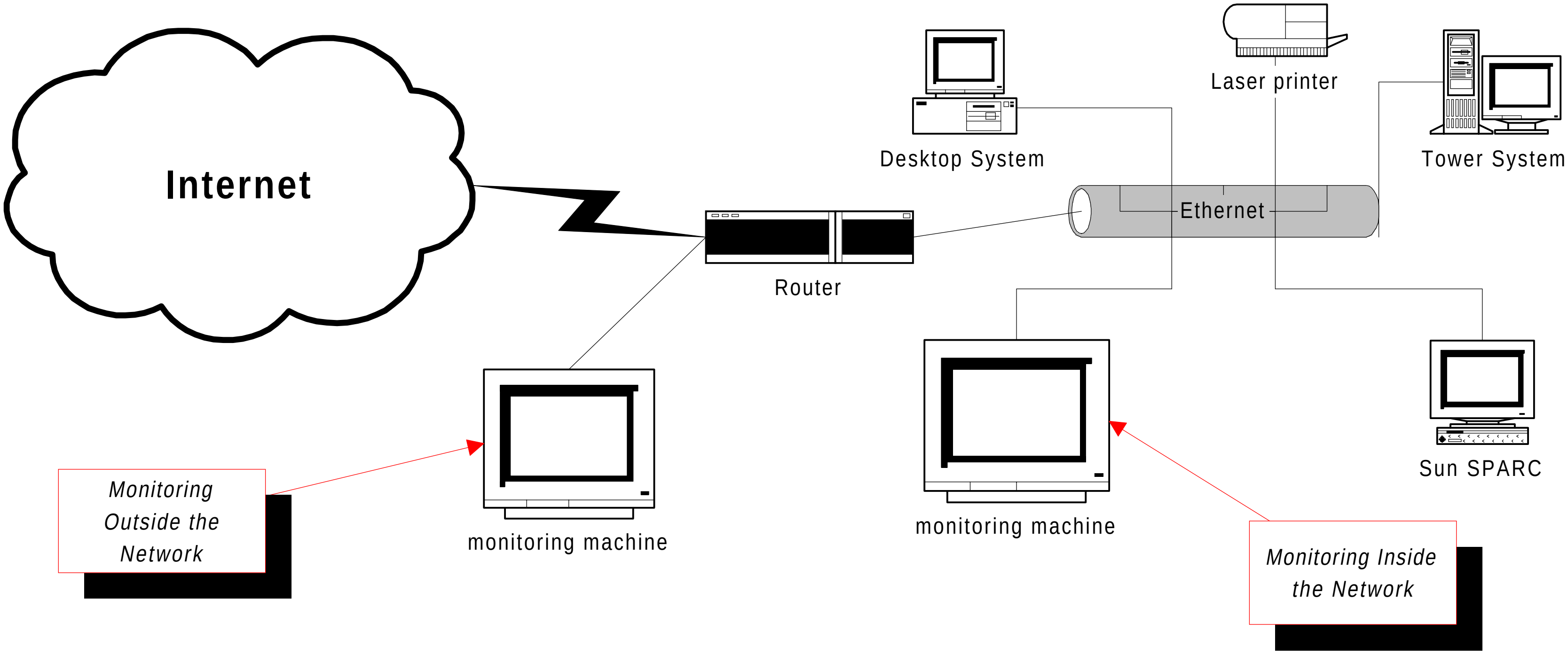
Where to Monitor - 1

- Common monitoring points
  - firewalls
  - routers
  - other access point (i.e. modems)
  - key network segments

Where to Monitor - 2

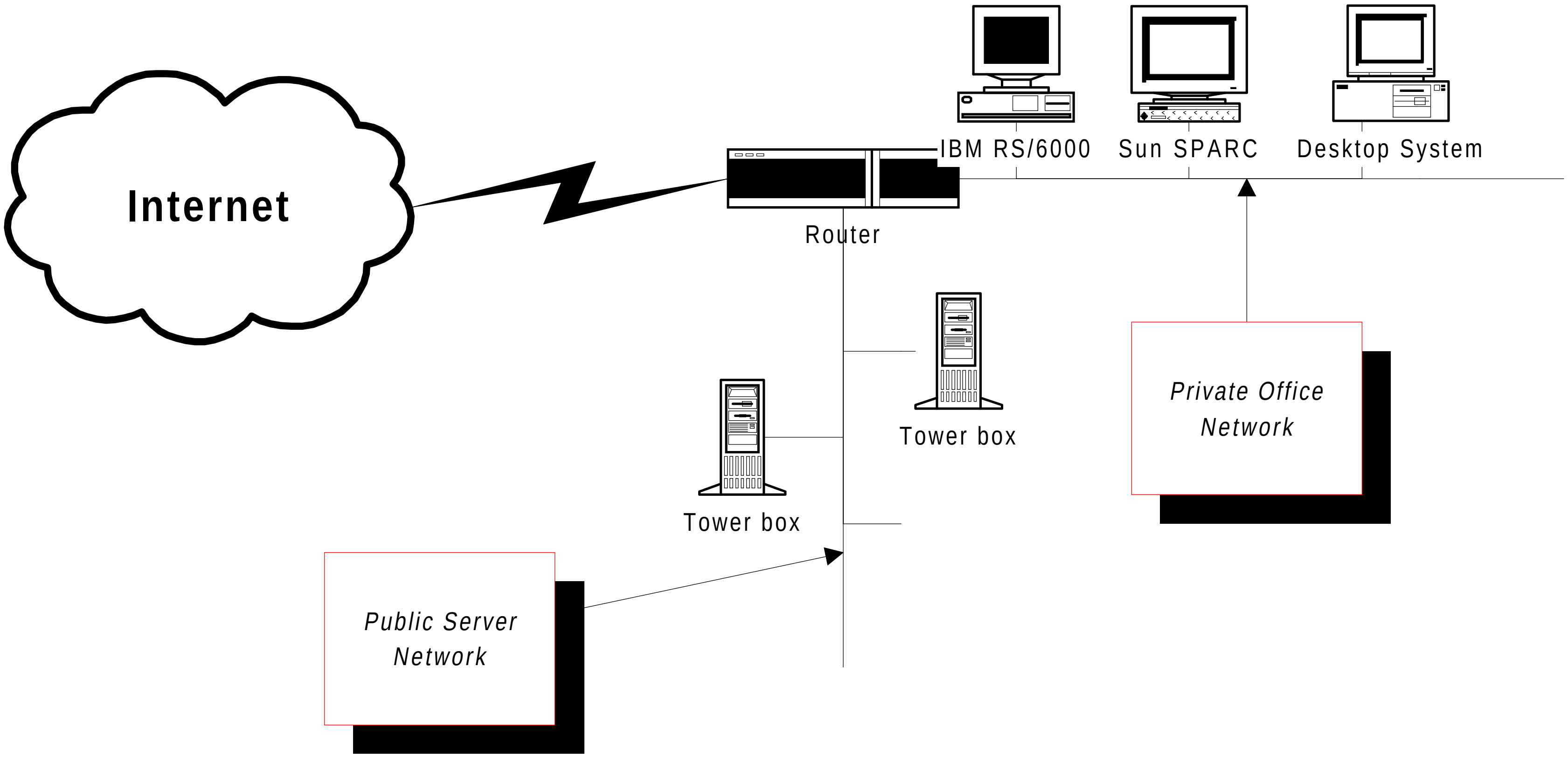
- Network traffic monitoring should be on an isolated machine
  - preservation of the integrity and security of monitoring machine is essential
  - compromise of the monitoring machine will compromise the integrity of logs

Where to Monitor - 3



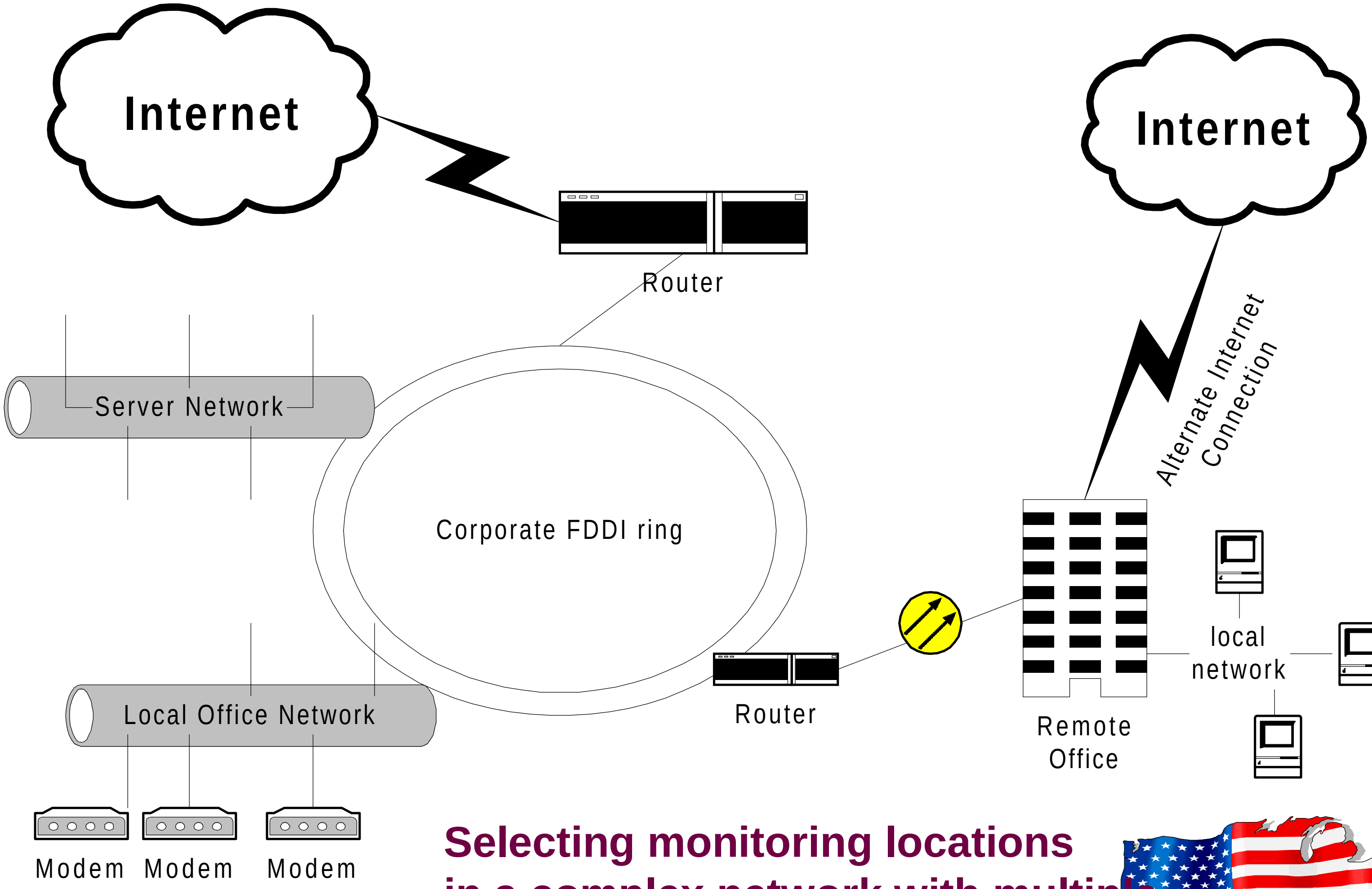
Monitoring inside and/or outside of your network

Where to Monitor - 4



Monitoring on different internal networks

Where to Monitor - 5



Selecting monitoring locations in a complex network with multiple access points

Types of Monitoring

- Connection monitoring
- Packet monitoring
- Detection
- Detection of new machines on your network

Intruder and User Profiling

- Intruder Profiling
  - looking for network activity that fits the profile of intruder activity
- User Profiling
  - looking for activity that does not fit the profile of normal user activity
- There are several commercial products that use profiling techniques.

Connection Monitoring

- Used to
  - log every connection or attempt to establish a connection
  - may be used to look for known intruder activity or suspicious activity

Packet Monitoring

- Used to
  - monitor individual packets on a subnet
  - log or decode packets
  - examine specific types of activity between specific machines
- Packet header monitoring vs. packet content monitoring

What to Look For in Your Log Files

- **Suspicious host connections**
- **Services being used during odd hours**
- **Changes in the behaviour of routers**
- **New hosts on your network**

Examples for Connection/Packet Monitoring

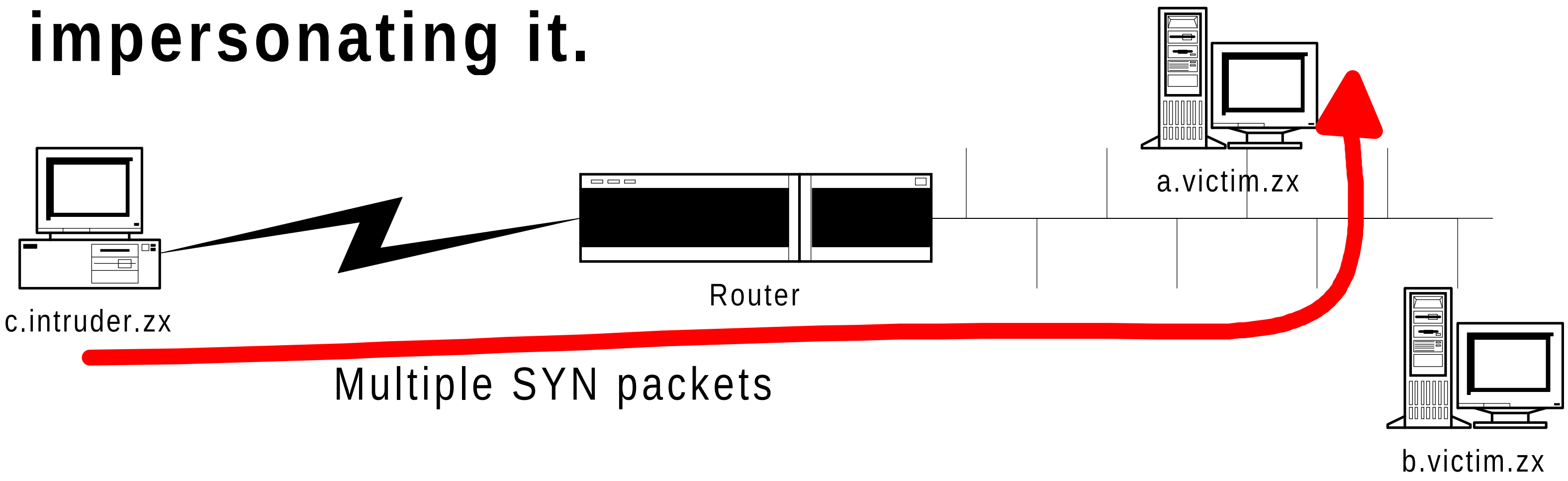
- Exploiting Berkeley “R” commands
- SYN denial of service attacks
- Brute force login attempts

Exploiting Berkeley “R” Commands - 1

- Exploits weaknesses in TCP/IP protocol and in TCP/IP implementations
- Exploits the weaknesses of authentication by IP address used by Berkeley “r” commands
  - rcp
  - rsh
  - rlogin

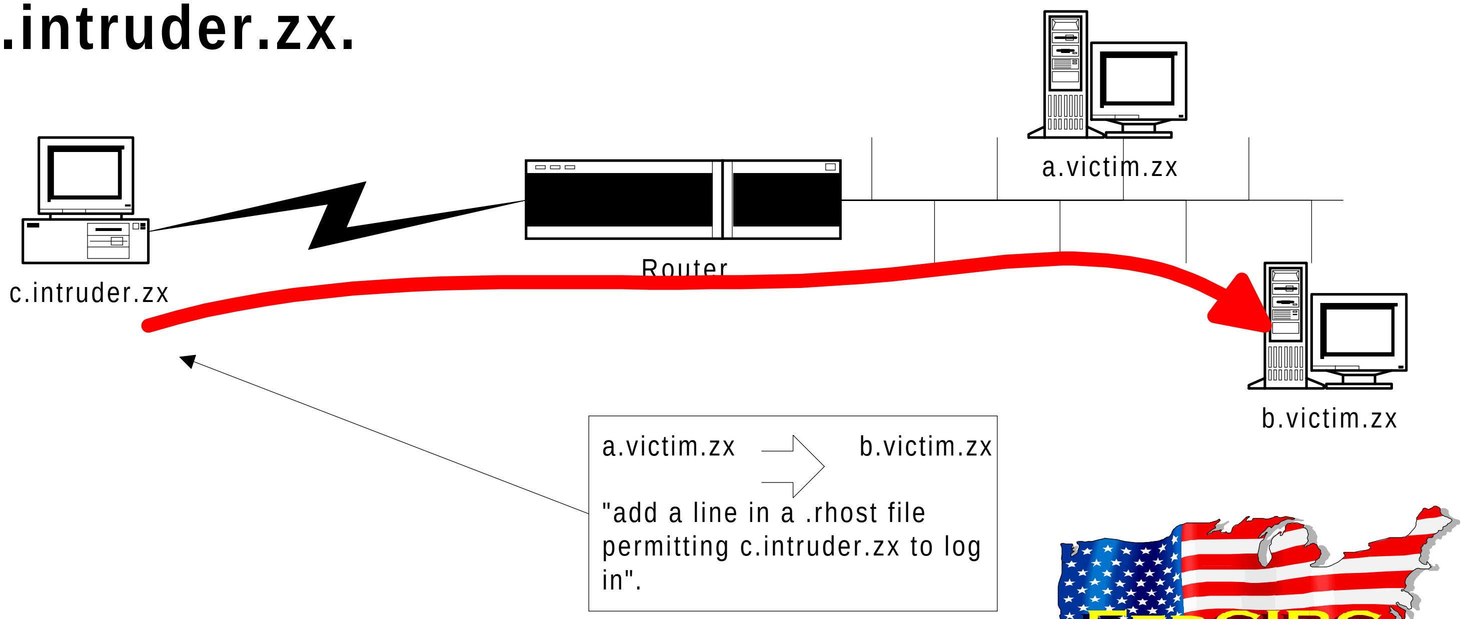
Exploiting Berkeley “R” Commands - 2

Step 1: Send SYN packets to a.victim.zx to "silence" it, in preparation for impersonating it.



Exploiting Berkeley “R” Commands - 3

Step 2: Send packets to b.victim.zx that appear to come from a.victim.zx. These packets will add an entry into a host.equiv or .rhosts file, allowing the intruder to then connect to b.victim.zx from c.intruder.zx.

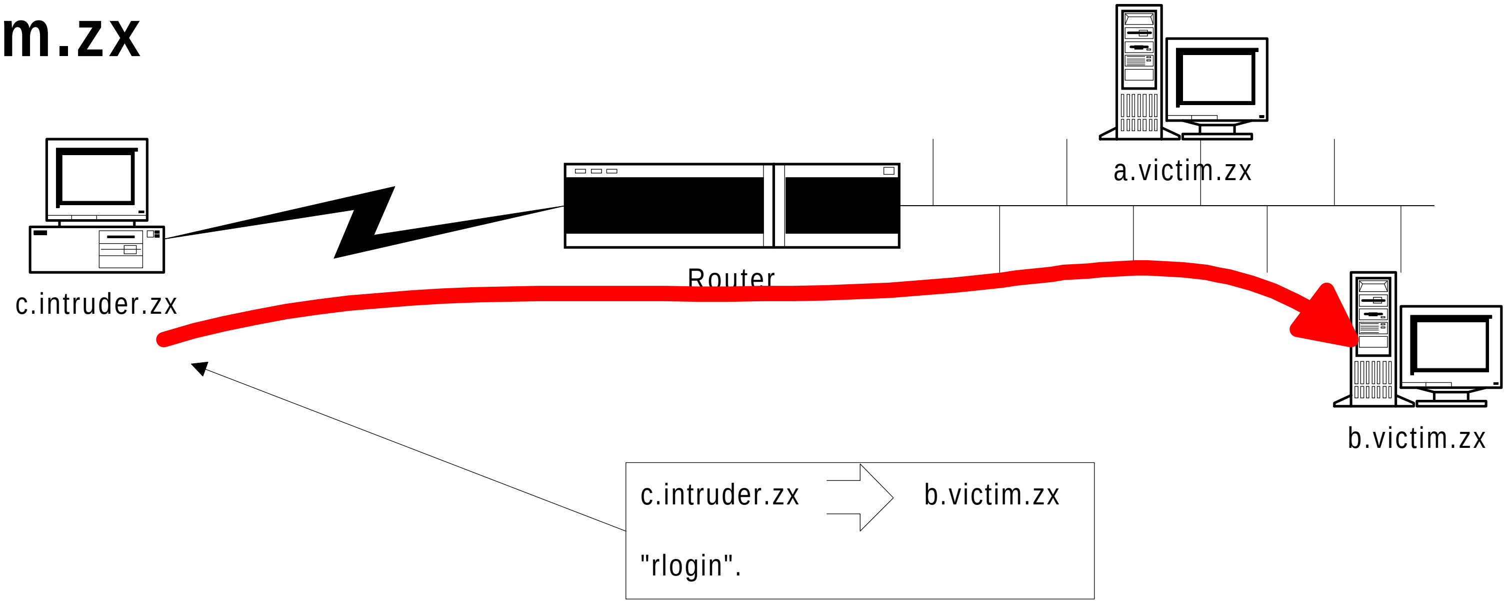


a.victim.zx ⇒ b.victim.zx

"add a line in a .rhost file permitting c.intruder.zx to log in".

Exploiting Berkeley "R" Commands - 4

Step 3: c.intruder.zx logs into b.victim.zx using the .rhost file now located on b.victim.zx



Exploiting Berkeley “R” Commands - 5

Monitoring can help by

- detecting SYN packets to a host
- detecting spoofed “r” packets to a host
- detecting “r” connections from remote hosts

Exploiting Berkeley “R” Commands - 6

Argus Logs:

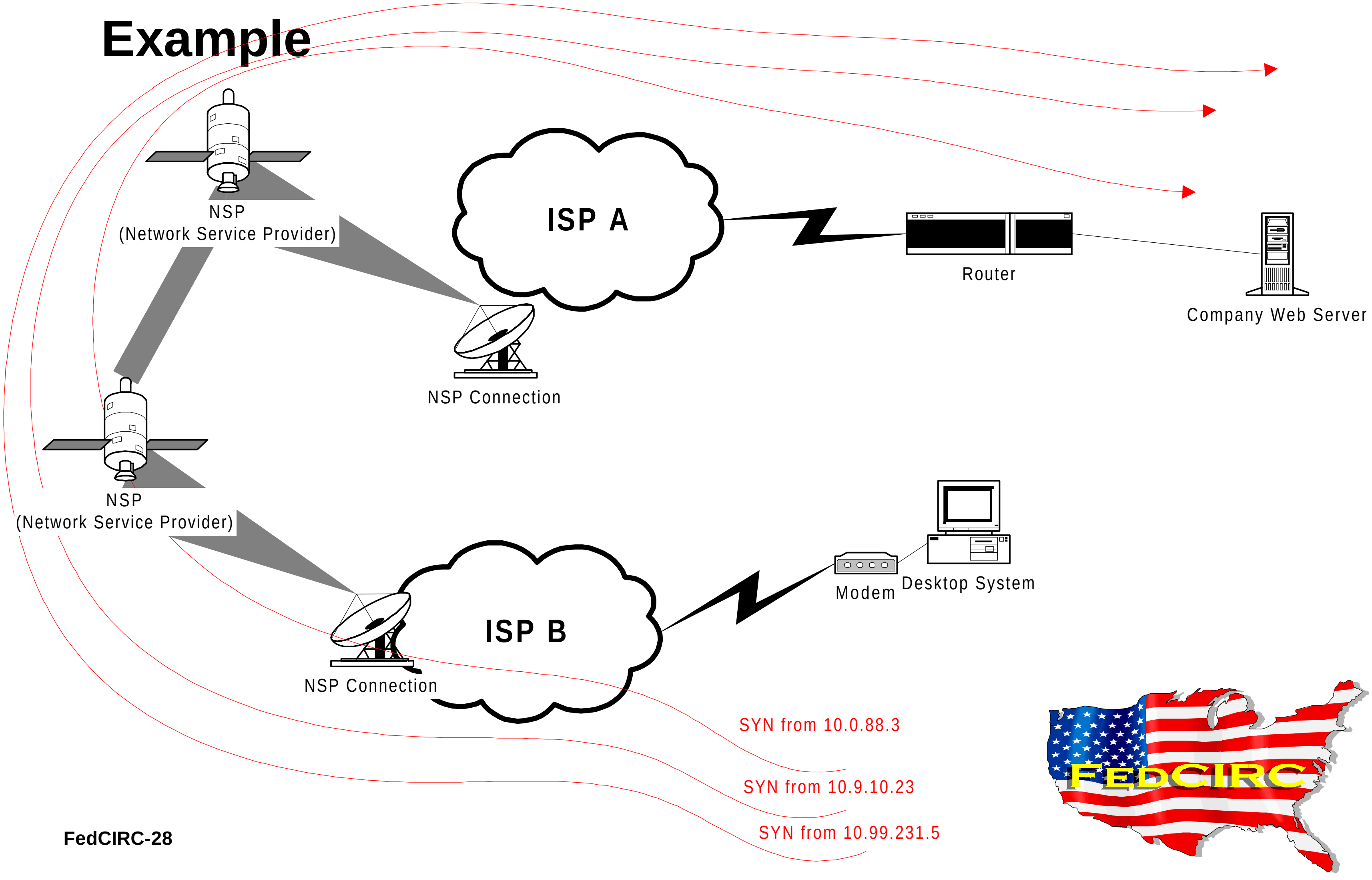
```
DATE      TIME     PROTOCOL          HOST.PORT   DIRECTION     HOST.PORT    STATUS
========= ========   ========   ================   ===       ==============   ======
Sun 12/24 19:47:32     tcp      19.17.14.17.600    |>        cert.org.login      RST
Sun 12/24 19:47:32     tcp      19.17.14.17.601    |>        cert.org.login      RST
Sun 12/24 19:47:32     tcp      19.17.14.17.602    |>        cert.org.login      RST
Sun 12/24 19:47:32     tcp      19.17.14.17.603    |>        cert.org.login      RST
Sun 12/24 19:47:32     tcp      19.17.14.17.604    |>        cert.org.login      RST
[ . . . ]
Sun 12/24 19:47:33     tcp      19.17.14.17.677    |>        cert.org.login      RST
Sun 12/24 19:47:33     tcp      19.17.14.17.678    |>        cert.org.login      RST
Sun 12/24 19:47:33     tcp      19.17.14.17.679    |>        cert.org.login      RST
Sun 12/24 19:47:37     tcp  XXXX.XXXXXXX.XX.shell  |>        cert.org.login      RST

Sun 12/24 19:49:40     tcp      19.17.14.17.600    |>        cert.org.login      RST
Sun 12/24 19:49:40     tcp      19.17.14.17.601    |>        cert.org.login      RST
Sun 12/24 19:49:40     tcp      19.17.14.17.603    |>        cert.org.login      RST
[ . . . ]
Sun 12/24 19:49:41     tcp      19.17.14.17.677    |>        cert.org.login      RST
Sun 12/24 19:49:41     tcp      19.17.14.17.678    |>        cert.org.login      RST
Sun 12/24 19:49:41     tcp      19.17.14.17.679    |>        cert.org.login      RST
Sun 12/24 19:49:45     tcp  XXXX.XXXXXXX.XX.shell  |>        cert.org.login      RST
```

SYN Denial of Service Attacks - 1

- Exploit weaknesses in the TCP/IP protocol and in TCP/IP implementations
- Typically use “spoofed” IP packets making it difficult to determine the source
- Can be difficult to trace the source of this type of attack

SYN Denial of Service Attacks - 2

Example



SYN Denial of Service Attacks - 3

Monitoring can help by

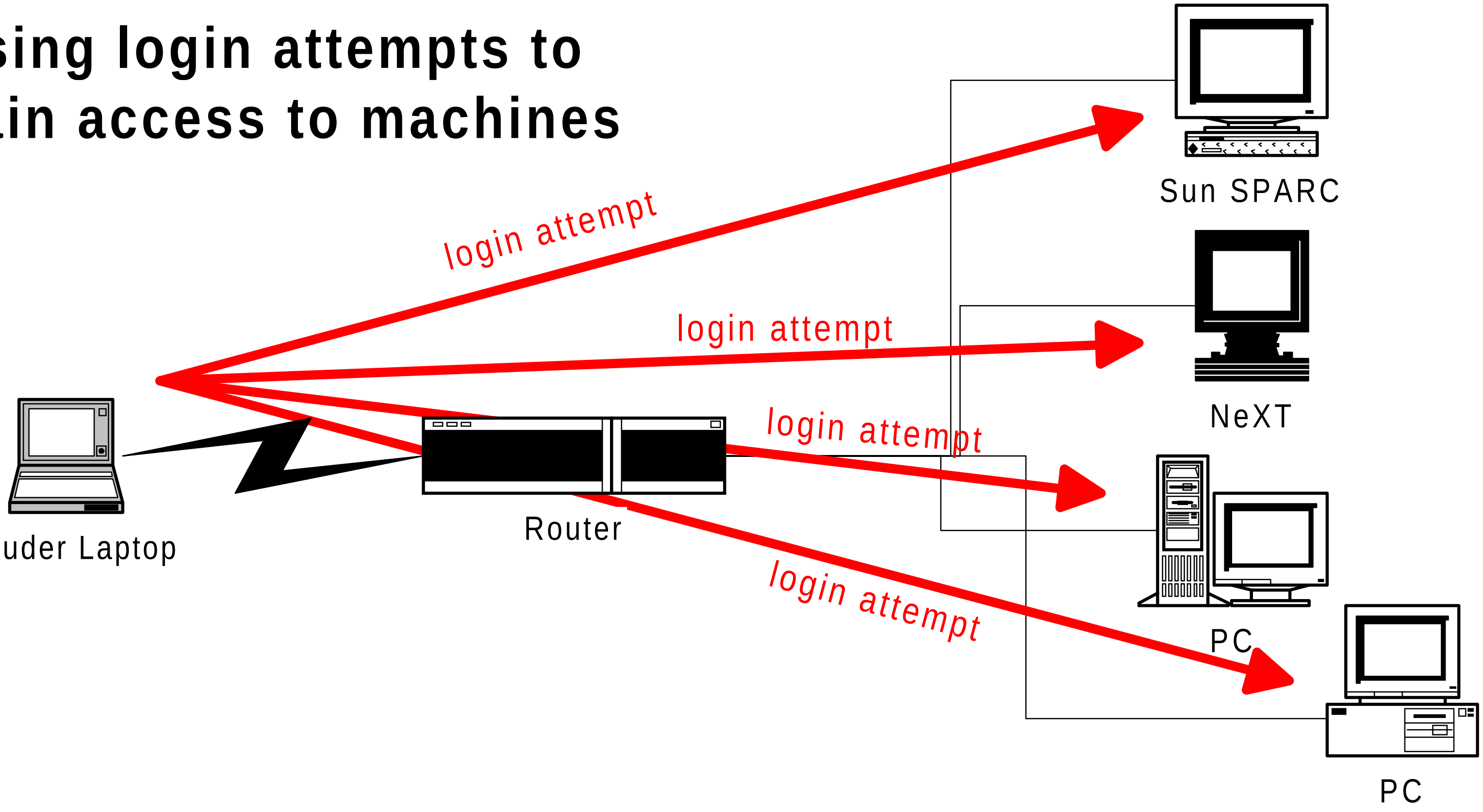
- detecting abnormally high numbers of connection attempts
- alerting system administrators to the activity

Login Attempts - 1

- Try to gain access to machines
- Use common, guessed, or cracked passwords
- Access accounts without passwords
- Attempt access on multiple machines

Login Attempts - 2

Using login attempts to gain access to machines



Login Attempts -3

Monitoring can help by

- Detecting higher than normal amount of login attempts
  - by origination machine
  - by number of target machines

Network Monitoring Tools

- Intrusion detection
  - NID

Network Intrusion Detector (NID) - 1

- URL: http://ciac.llnl.gov/cstc (NID is freely available to all U.S. Government agencies, and to contractors directly supporting the U.S. Departments of Defense and Energy.)
- Description: NID is a suite of software tools that helps detect, analyze, and gather evidence of intrusive behavior networks. NID is directly connected to the local area network it protects and it collects packets or statistics that cross a user-defined security domain. When threat patterns are recognized, NID signals the event locally and can save the suspicious session for later analysis or playback.

Network Intrusion Detection (NID) - 2

- **Author: Computer Security Technology Center, Lawrence Livermore National Laboratory**

Network Monitoring Tools

- Connection monitoring
  - argus
  - netlog
  - clog
  - nfswatch

argus

- URL: ftp://ftp.sei.cmu.edu/pub/argus-1.5
- Description: Argus is a generic IP network transaction auditing too. Argus runs as an application level daemon, promiscuously reading network data grams from a specified interface, and generates network traffic status records for the network activity it encounters.
- Current Version:1.5
- Authors: Carter Bullard and Chas DiFatta (Software Engineering Institute)

netlog - 1

- URL: ftp://net.tamu.edu/pub/security/TAMU
- Description: This is a TCP and UDP traffic logging system. Logfiles can be processed to look for suspicious activity.
- Current Version: 1.2
- Author: Texas A&M University

netlog - 2

- Part of the TAMU security package
- Netlog only works on Sun workstations
- Netlog contains five separate programs
  - tcplogger: log all tcp connections on a subnet
  - udplogger: log all udp sessions on a subnet
  - icmplogger: log icmp messages on a subnet
  - extract: process log files produced by tcplogger and udplogger
  - netwatch: real time network monitor

clog - 1

- URL: ftp://coast.cs.purdue.edu/pub/tools/unix/clog
- Description: Clog is very similar in functionality to the tcplogger tool in the TAMU netlog package. Clog uses libpcap and compiles on most Unix implementations.
- Current Version: 1.5
- Author: Brian Mitchell <brian@saturn.net>

clog - 2

clog sample output

```
Date|Source Host|Source Port|Destination
  Host|Destination Port

Mar 16 11:30|your.host.gov|1831|time.sync.gov|37
Mar 16 11:35|school.edu|1199|your.host.gov|25
Mar 16 12:00|intruder.zx|1023|your.host.gov|22
Mar 16 12:29|your.host.gov|1856|rs5.internic.net|43
```

nfswatch - 1

- URL: ftp://coast.cs.purdue.edu/pub/tools/unix/nfswatch
- Description: Nfswatch monitors NFS requests to any given machine, or the entire local network. This program is useful for the purpose of detecting attempted NFS intrusions on your network.
- Current Version: 4.2
- Authors: Dave Curry (Purdue University) and Jeff Mogul (Digital Equipment Corporation)

nfswatch - 2

- nfswatch is useful in addition to other connection monitoring tools because NFS data is decoded from UDP packets.

Network Monitoring Tools

- Packet monitoring
  - tcpdump
  - snoop
  - there are a number of commercial Packet Monitoring tools.

tcpdump - 1

- URL: ftp://ftp.ee.lbl.gov/tcpdump.tar.Z
- Description: Tcpdump is a tool for network monitoring and data acquisition. Data from individual packets can be logged and processed by other programs.
- Current Version: 3.3
- Author: Lawrence Berkeley National Laboratory (Network Research Group)

tcpdump - 2

tcpdump sample default output

```
Time (Source Host.Source Port) > (Destination
  Host.Destination Port): More packet info
15:03:03.410000 outside.host.zx.1023 > your.host.gov.22:
   . ack 1868333138 win 8960 (DF) [tos 0x10]
15:03:03.470000 your.host.gov.22 > outside.host.zx.1023:
   P 1:45(44) ack 0 win 31744 (DF) [tos 0x10]
15:03:03.710000 outside.host.zx.1023 > your.host.gov.22:
   . ack 45 win 8960 (DF)[tos 0x10]
15:03:05.190000 outside.host.zx.1023 > your.host.gov.22:
   P 0:20(20) ack 45 win 8960 (DF) [tos 0x10]
```

tcpdump - 3

- Output is configurable
- You can filter for suspicious hosts
- All data that travels your network can be logged by tcpdump into a file and processed at a later date.

snoop - 1

- **Description: Snoop is a utility used to capture and decode packets from the network and display their contents. Captured packets can be displayed as they are received, or saved to a file for later inspection.**
- **Note: Snoop is a utility included with the the Solaris distribution since version 2.3.**
- **There are similar commercial products to capture and decode packets which work on other operating systems.**

snoop - 2

- Snoop can be used to monitor and decode suspicious connections in real time
- Snoop can log all network traffic to a file for later inspection

synsniff - 1

- URL:
  ftp://coast.cs.purdue.edu/pub/tools/unix/synsniff.tar.gz
- Description: synsniff is a perl script which uses tcpdump to watch and log all inbound connections to a network. synsniff will also attempt to identify port scans and flag them as such.
- synsniff is essentially an interface to tcpdump to provide a connection logging mechanism that also looks for port scans.
- Current Version: 0.4b
- Author: James W. Abendschan <jwa@nbs.nau.edu>

synsniff - 2

synsniff sample output

```
03/15 14:35:05 tcp intruder.zx :4995 -> your.host.gov:21
03/15 14:35:06 tcp intruder.zx :20503 -> your.host.gov :23
03/15 14:35:12 tcp intruder.zx :32079 -> your.host.gov :25
03/15 14:35:12 tcp intruder.zx :22165 -> your.host.gov :79
03/15 14:35:12 tcp intruder.zx :27945 -> your.host.gov :119
03/15 14:35:12 tcp intruder.zx :3170 -> your.host.gov :139
   [PORTSCAN]
```

Automated Scanning - 1

- Port scanning is used by intruders to determine what services you are running on your host
- Connection and packet monitoring tools can be used to detect automated port scanning
- A large number of SYN (connection request) packets on several ports in a short amount of time can be an indication of port scanning.
- Port scanners generally operate incrementally (i.e. port 1,2,3, etc…), but this may not always be the case

Automated Scanning - 2

- Tools like SATAN (System Administrators Tool for Analyzing Networks) allow automated vulnerability scanning of networks.
- Detection of such activity requires software to look for patterns of scanning in tools like SATAN.

Automated Scanning - 3

- **Sample port scan log from clog**

```
Mar 16 23:55|intruder.zx|1183|your.host.gov|1
Mar 16 23:55|intruder.zx|1185|your.host.gov|2
Mar 16 23:55|intruder.zx|1187|your.host.gov|3
Mar 16 23:55|intruder.zx|1188|your.host.gov|4
Mar 16 23:55|intruder.zx|1189|your.host.gov|5
Mar 16 23:55|intruder.zx|1190|your.host.gov|6
Mar 16 23:55|intruder.zx|1191|your.host.gov|7
Mar 16 23:55|intruder.zx|1192|your.host.gov|8
Mar 16 23:55|intruder.zx|1193|your.host.gov|9
Mar 16 23:55|intruder.zx|1194|your.host.gov|10
Mar 16 23:55|intruder.zx|1195|your.host.gov|11
```

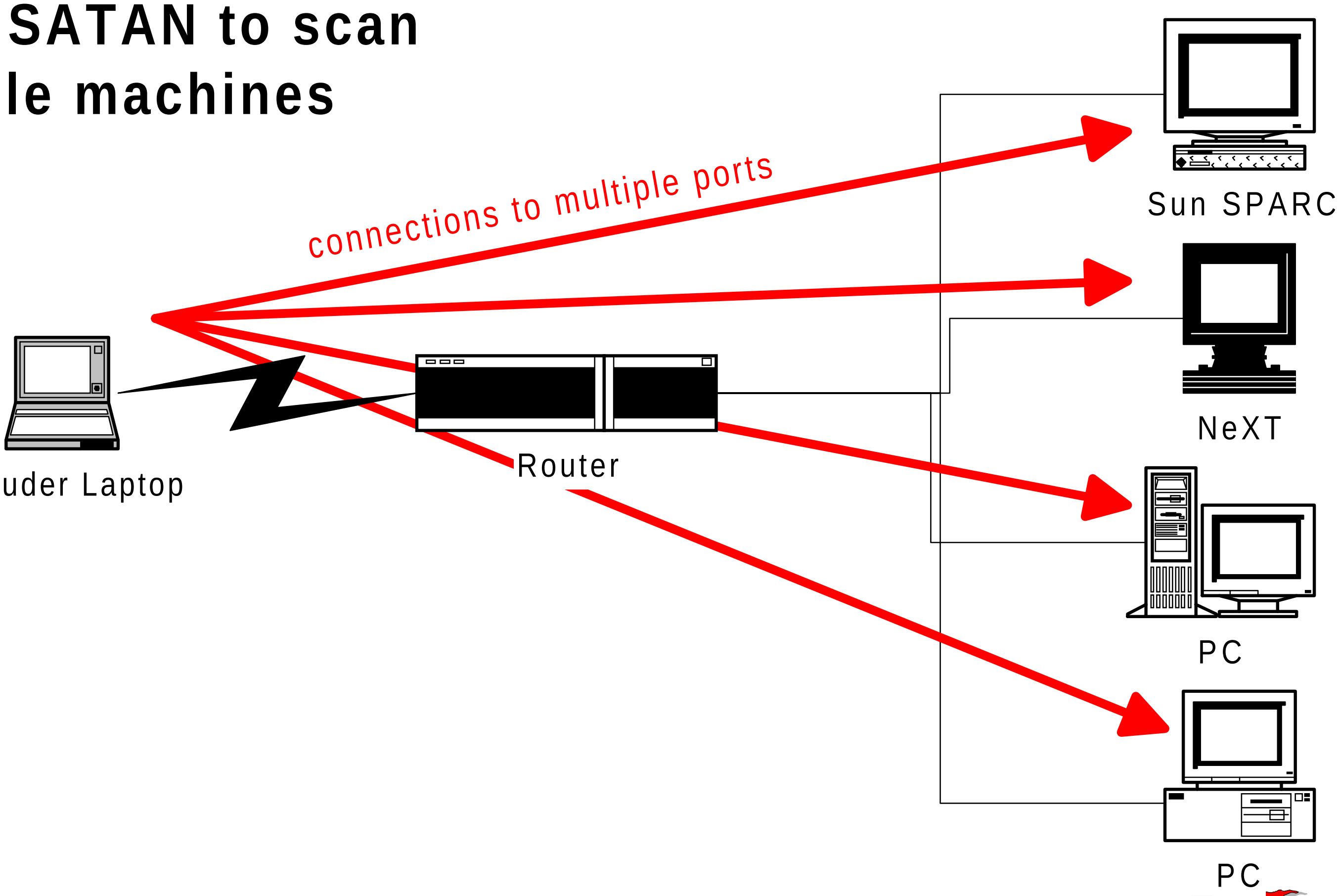
etc......

SATAN Scans - 1

- Probe network services on hosts looking for known vulnerabilities
- Provide the intruders with a list of machines that are vulnerable to a compromise

SATAN Scans - 2

Using SATAN to scan multiple machines



SATAN Scans - 3

Monitoring can help by

- detecting that machines are being probed for vulnerabilities
  - some hosts may not be aware they are being probed
  - network monitoring can be used to determine scope of scans
- observe the origin of the scanning attempts

Network Monitoring Tools

- Detecting automated scanning
  - courtney
  - gabriel

courtney - 1

- URL: http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html
- Description: Courtney monitors the network and identifies the source machines of SATAN probes/attacks. Courtney receives input from tcpdump counting the number of new services a machine originates within a certain time window. If one machine connects to numerous services within that time window, Courtney identifies that machine as a potential SATAN host.
- Current Version: 1.3
- Author: CIAC

courtney - 2

Example syslog entries:

```
Mar 30 22:24:31 mercury courtney[2976]: HEAVY_ATTACK
  from a.intruder.zx - to b.victim.zx
Mar 30 22:24:32 mercury courtney[2976]: HEAVY_ATTACK
  from a.intruder.zx - to c.victim.zx
Mar 30 22:24:33 mercury courtney[2976]: HEAVY_ATTACK
  from a.intruder.zx - to d.victim.zx
```

gabriel

- URL: http://www.lat.com/gabe.htm
- Description: Gabriel gives the system administrator an early warning of possible network intrusions by detecting and identifying network probing. Gabriel only works with Solaris.
- Current Version: 1.0
- Author: Los Altos Technologies

Detecting new machines on your network

- The physical security of your network is important
- The addition of new machines may compromise the security of your network
- New machines can be detected by
  - network monitoring machines
  - routers
  - firewalls

Network Monitoring Tools

- Detection of new machines on your network
  - arpwatch

arpwatch

- URL: ftp://ftp.ee.lbl.gov/arpwatch.tar.Z
- Description: Arpwatch is a tool that monitors ethernet activity and keeps a database of ethernet/ip address mappings. Changes are reported by email. This is a very useful tool for detecting new machines on a network.
- Current Version: 2.0
- Author: Lawrence Berkeley National Laboratory (Network Research Group)

Topics

- Network monitoring
- ➤ Firewalls
- Routers

Firewalls - 1

- Extensive and configurable logging is necessary
- Firewall logs can be vital in detecting intrusions
- Firewalls set the baseline for ID activities

Firewalls - 2

- Commercial firewalls
  - http://www.firewall.com
- Freeware firewalls
  - TAMU DrawBridge
    - ftp://net.tamu.edu/pub/security/TAMU
  - TIS Firewall Toolkit - FWTK
    - ftp://ftp.tis.com/pub/firewalls/toolkit
- For more information on firewalls see
  - http://www.v-one.com/pubs/fw-faq/faq.htm

Topics

- Network monitoring
- Firewalls
- Routers

Routers

- Threats
  - Compromised administrative account
  - Denial of Service
    - Spoofed RIP packets
    - Spoofed ICMP redirects
    - Spoofed ICMP destination unreachable
  - Redirection of network traffic

Detecting intrusions on routers

- Denial of service attacks can result in a loss of connectivity
- Verify the integrity of the router configuration file
- Audit the log files produced by the router

Router Configuration Files

- **Regularly verify the integrity of router configuration files**
- **Regularly check the security of the host serving configuration files**

Conclusion

- Connection monitoring is an important supplement to host-based monitoring.
- It is important to understand your network topology in order to effectively monitor.
- A number of tools are available to assist network administrators in implementing monitoring.

Bibliography

- Cheswick, W. R., and Bellovin, Steven M., *Firewalls and Internet Security*, Addison-Wesley Publishing Co., Reading, Massachusetts, 1992.
- White, Gregory B., Fisch, Eric A., Pooch, Udo W., *Computer System and Network Security*, CRC Press, Boca Raton, Florida, 1996.
- Kaufman, Charlie, Perlman, Radia, Speciner, Mike, *Network Security PRIVATE Communication in a PUBLIC World*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1995.

Bibliography - 2

- Pfleeger, Charles P., *Security in Computing Second Edition*, Prentice Hall PTR, Upper Saddle River, New Jersey,1997.
- Chapman, D. Brent, Zwicky, Elizabeth D., *Building Internet Firewalls*, O'Reilly & Associates, Inc. Sebastopol, California, 1995.
- Hare, Chris, Siyan, Karanjit, *Internet Firewalls and Network Security Second Edition*, New Riders Publishing, Indianapolis, Indiana, 1996.